



MARY KAY O'CONNOR PROCESS SAFETY CENTER

TEXAS A&M ENGINEERING EXPERIMENT STATION

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Considering Multiple Initiating Events in a LOPA

Denise Chastain-Knight, PE, CFSE, CCPSC

Loren Stewart, CFSE

exida

80 North Main Street

Sellersville, PA, 18960, USA

Emails: dchastainknight@exida.com, lstewart@exida.com

Keywords: Semiquantitative Risk Assessment, Layer of Protection Analysis (LOPA), Interlocks & Safety, Safety Instrumented Systems (SIS), Residual Risk Management, Alarm and Instrument Management, Automatic SIS System

Abstract

Layer of Protection Analysis (LOPA) is a risk reduction evaluation methodology well suited to consider hazard scenarios with multiple initiating events. The presence of multiple initiators increases the likelihood that a hazard scenario could occur placing additional demands on the Independent Protection Layers (IPLs) that prevent and mitigate the hazard. This paper will discuss the impact of multiple initiating events on demand frequency, discuss methods to evaluate the effectiveness of IPLs, and determine which may be considered to reduce the demand on a Safety Instrumented Function (SIF) and Safety Integrity Level (SIL) targeting. Finally, the impact of demand frequency and proof test interval on SIF demand mode will be illustrated.

Introduction

The Layer of Protection Analysis (LOPA) was developed nearly twenty years ago to fill the gap between qualitative process hazard analysis (PHA) and detailed quantitative risk analysis (QRA). The objective of a LOPA is to determine what PHA safeguards serve as Independent Protection Layers (IPL) and confirm risk is reduced to as low as reasonably practicable (ALARP)¹ levels. When a Safety Instrumented Function (SIF) is one of the IPLs, the LOPA is also used to determine Safety Integrity Level (SIL) and SIF demand frequency. When used thoughtfully, much more information can be captured by the LOPA that is required for specification and design of a SIF. LOPA will also document key information later needed for Safety Requirements Specification (SRS) including:

- Demand source
- Demand frequency
- Additional mitigation
- Risk receptors
- Related interlock

LOPA Presentation

LOPA may be presented in many different formats. Figure 1 illustrates some common formats including portrait format summary (A), event tree (B), and landscape format summary (C).

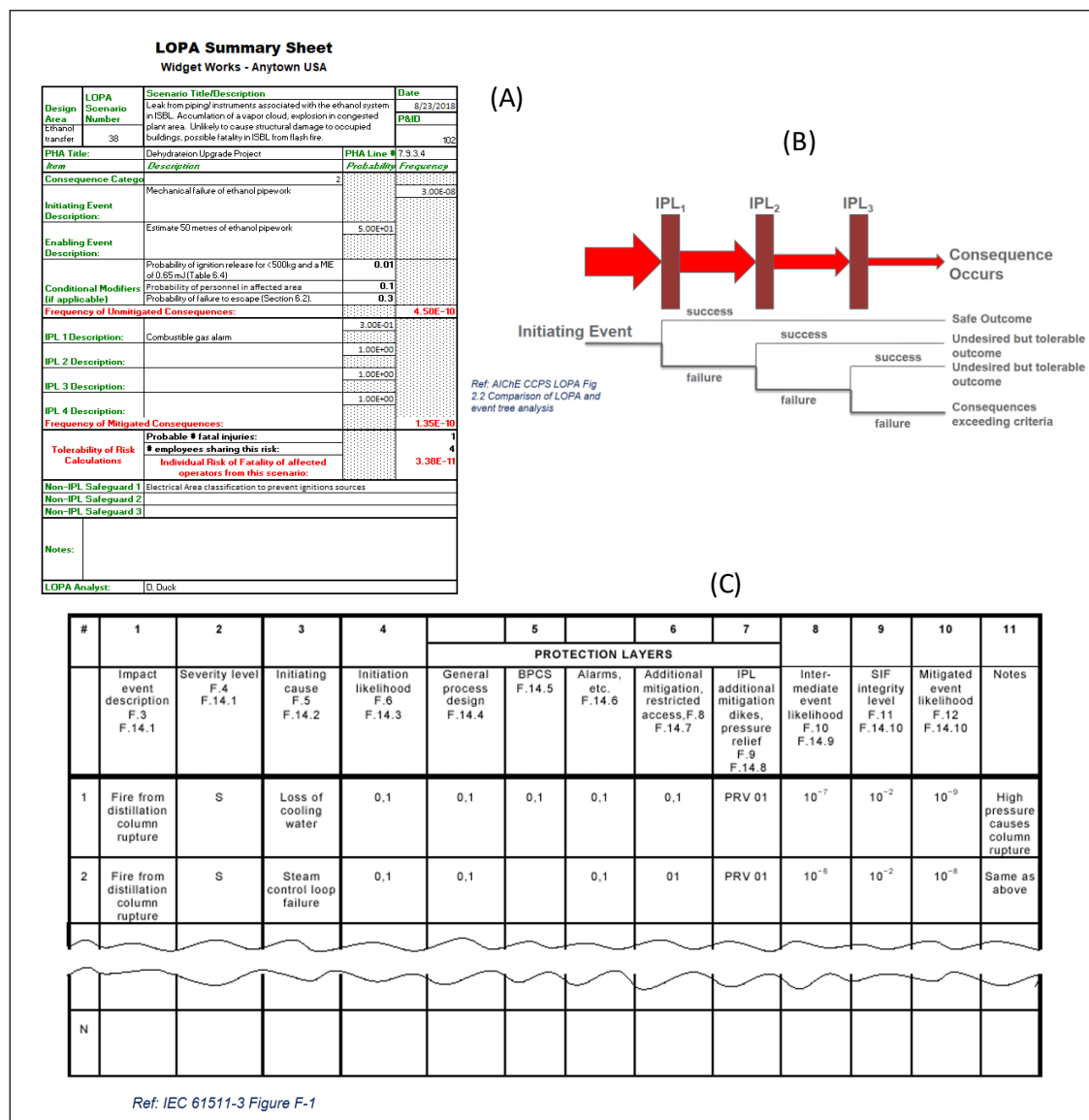


Figure 1 – Common LOPA Presentations

Figure 1A is consequence based and captures a lot of information including identification of multiple initiating events and IPLs, but it does not provide a framework to assess the effectiveness of IPLs against individual initiators or risk receptors. Figure 1B is initiating event focused, provides a detailed analysis of the effectiveness of IPLs against the initiator, identifies multiple potential outcomes for an event and delivers some risk receptor information. Figure 1C is cause/consequence pair based focusing analysis on one branch of the event tree. All of these methods consider a worst case tolerable frequency regardless of risk receptor (e.g. safety, environment, business) for the analysis.

This paper will utilize a LOPA format that considers multiple initiators in a single view and provides a framework to analyze the effectiveness of IPLs against individual initiators, separately for each risk receptor (Figure 2)².

(B) (G) (H)												
Target Frequency	Actual Frequency	RRF										
B 0.01	3.18E-4	NA										
E 0	0.2	NA										
S 1.00E-3	3.18E-4	NA										
			(D)									
8. SIF 001: High temperature from Crude Heater												
(A)			Frequency [per year]	ECs	IPLs			CMs			Intermediate Frequency [per year]	Comments
Initiating Event				Manual setpoint entry requires supervisor key	TAHH-3100 Fractionator Sump	SIF001 Heater H-100 shutdown	(I)	Column damage only occurs at high temperature for a long time.			(F)	
Higher temperature crude from heater H-100 than required - human error set point incorrect to TIC-1000 or FIC-1001 in manual	0.1	B	0.25	B	NA	B	9.09E-2	B	0.1	B	2.27E-4	
		E	NA	E	(E)	E	NA	E	NA	E	0.1	
		S	0.25	S		S	9.09E-2	S	0.1	S	2.27E-4	
Higher temperature crude from heater H-101 than required control failure TIC-1000	0.1	B	NA	B	0.1	B	9.09E-2	B	0.1	B	9.09E-5	
		E	NA	E	NA	E	NA	E	NA	E	0.1	
		S	NA	S	0.1	S	9.09E-2	S	0.1	S	9.09E-5	

Figure 2 – exSILentia Framework

The LOPA is named (A) to represent the undesired consequence and may contain identifiers for the SIF intended to protect against the consequence. The tolerable target frequency of consequence for each risk receptor is defined in the summary table (B) at the top of Figure 2. Initiating events are presented in rows of the analysis table (C) with sub-rows for each risk receptor. Columns are grouped (left to right) by enabling conditions (EC), IPLs and Conditional Modifiers (CM) (D). Within the IPL subgroup, the IPLs are positioned in the sequence in which they are effective. For example, if the intended protection layer sequence is operator response to a process alarm, SIF action, then relief device actuation, IPLs would be placed in this order. The software interprets the sequencing to indicate which IPLs act to reduce demand (alarm) on the SIF and those that do not (relief). Probability of failure on demand (PFD) for the EC, IPL and CM layers are recorded in a background database and are applied where the user indicates effectiveness against initiating events (E). Intermediate frequency is calculated for each IE by risk receptor (F), and cumulative frequency is tallied by risk receptor in the summary table (G). The RRF column of the summary table indicates a gap between tolerable risk and scenario risk (H). Once PFD data is entered for all non-SIF IPLS, and protection has been assigned, target SIL may be calculated for the SIF (I). From this arrangement the information which may be extracted for the SRS includes:

- Demand source – Description of initiating events with individual frequencies.
- SIF Demand frequency – Calculated from individual demand frequencies considering EC and IPLs that reduce demand.
- Additional mitigation – Complete list of IPLs that provides mitigation, ECs and CM that could be managed through other means.
- Risk receptors – Summary by receptor provide information that could impact design decisions.
- Related interlock – Processes may have interlocks in DCS, package equipment and SIS. Each is indicated by a separate IPL.

- SIL Target – Directly calculated including residual risk.

LOPA Evaluation as Individual Records

When a LOPA does not consider multiple initiating events in a combined analysis, the SIL target and demand frequency can be underestimated, thus resulting demand mode may be misjudged. The following example considers three records extracted from a HAZOP for scenarios where the consequence of concern is a loss of pilots to a fired heater, with the potential for fire/explosion. The event consequence was determined to have a tolerable frequency of 1E-4 for business interruption, 1E-2 for environmental consequence and 1E-3 for safety. Figure 3 illustrates a cause/consequence pair for a human error initiating event (cause 1). The valve is remotely located, so an enabling condition regarding accessibility of the valve is included to reduce the likelihood of this initiating event. Potential IPLs identified from the HAZOP safeguards are listed as a group. The PFD for the IPLs is entered in a database and assigned individually to each risk receptor, where they are effective. After all information is entered, the SIF PFD is calculated to close the gap between intermediate frequency and tolerable frequency. This analysis suggests the SIF should be a SIL 1 target RRF of 10 ($RRF = 1/PFD = 1/0.1$) with a demand frequency of 0.01/year ($f_{IE} * f_{EC}$).

Target Frequency	Actual Frequency	RRF		
B 1.00E-4	1.00E-4	NA		
E 1.00E-2	1.00E-4	NA		
S 1.00E-3	1.00E-4	NA		


3. Loss of Pilots Heater Trip - Cause 1		Frequency [per year]	Likelihood of personnel working in area where valve is located	IPLs				Intermediate Frequency [per year]
Initiating Event				Cause 1 SIF	PAL-123 Natural Gas to Pilot line.	PAH-145 Firebox Pressure		
Battery Limit Natural Gas Ball Valve inadvertently closed.		0.1		B 0.1	B 1.00E-1	B 0.1	B NA	B 1.00E-4
				E 0.1	E 1.00E-1	E 0.1	E NA	E 1.00E-4
				S 0.1	S 1.00E-1	S 0.1	S NA	S 1.00E-4





Figure 3 - Cause 1

Figures 4 and 5 illustrate analysis for two additional cause/consequence pairs from the HAZOP record. Figures 3 and 4 both credit the pilot gas low pressure alarm for the operator response, but in Figure 5, the firebox high pressure is considered the more effective alarm. Only one alarm may be considered per IE because they reside in the same DCS, and are managed by the same operator (not independent).

Target Frequency	Actual Frequency	RRF	<div><div><div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div><div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div></div></div></div>										
B	1.00E-4	1.00E-4	NA										
E	1.00E-2	1.00E-4	NA										
S	1.00E-3	1.00E-4	NA										

4. Loss of Pilots Heater Trip - Cause 2			Frequency [per year]		IPLs						Intermediate Frequency [per year]	
Initiating Event					Cause 2 SIF		PAL-123 Natural Gas to Pilot line.		PAH-145 Firebox Pressure			
PCV-033 Natural Gas to Heater pilots fails.			0.1	<div><div></div><div></div><div></div></div>	B	1.00E-2	B	0.1	B	NA	B	1.00E-4
					E	1.00E-2	E	0.1	E	NA	E	1.00E-4
					S	1.00E-2	S	0.1	S	NA	S	1.00E-4

Figure 4 - Cause 2

Target Frequency	Actual Frequency	RRF	 ▶ 	
B	1.00E-4	NA		
E	1.00E-2	NA	 ▶ 	
S	1.00E-3	NA		


5. Loss of Pilots Heater Trip - Cause 3		Frequency [per year]	IPLs				Intermediate Frequency [per year]				
Initiating Event			Cause 3 SIF	PAL-123 Natural Gas to Pilot line.		PAH-145 Firebox Pressure					
Combustion chamber steam inadvertently opened		0.01		B	1.00E-1	B	NA	B	0.1	B	1.00E-4
			E	1.00E-1	E	NA	E	0.1	E	1.00E-4	
			S	1.00E-1	S	NA	S	0.1	S	1.00E-4	

Figure 5 - Cause 3

Each of the three LOPAs are anticipated to set the SIL target for the SIF. That will identify the loss of the pilot flame and bring the process to a safe state by tripping the fuel valves. Results of the analysis are summarized in below in Table 1.

Table 1 – Cause/Consequence Pair Analysis Summary

	SIL Target	SIF RRF target	Demand Frequency / year
Cause 1	1	10	0.01
Cause 2	2	100	0.1
Cause 3	1	10	0.01

So what is the design basis for the SIF? Frequently, causes are considered separately so the SIF design basis may be selected on the ‘worst case’ scenario without consideration for the cumulative impact of multiple causes. Cause 2 has the highest SIL target and the highest demand frequency so users might select this as the ‘worst case’ design basis. Simply selecting the case that delivers the highest target, ignores residual risk and multiple demands as illustrated by a combined LOPA evaluation.

Combined LOPA Evaluation

In SIF design, the user must consider the combined impact of multiple initiating events, the effectiveness of IPLs against each cause, and the cumulative effect on both demand and RRF requirements. Figure 6 is a combined LOPA which includes all three initiating events in a single analysis. The inset below the LOPA is a view of the SRS, where the demand rate is automatically populated by exSILentia based on the LOPA. Target frequency, initiating event frequency, EC and non-SIF IPLs are the same as given in the individual analysis. The EC/IPL effectiveness is noted the same as in Figures 3-5, then the SIL target for the SIF is calculated.

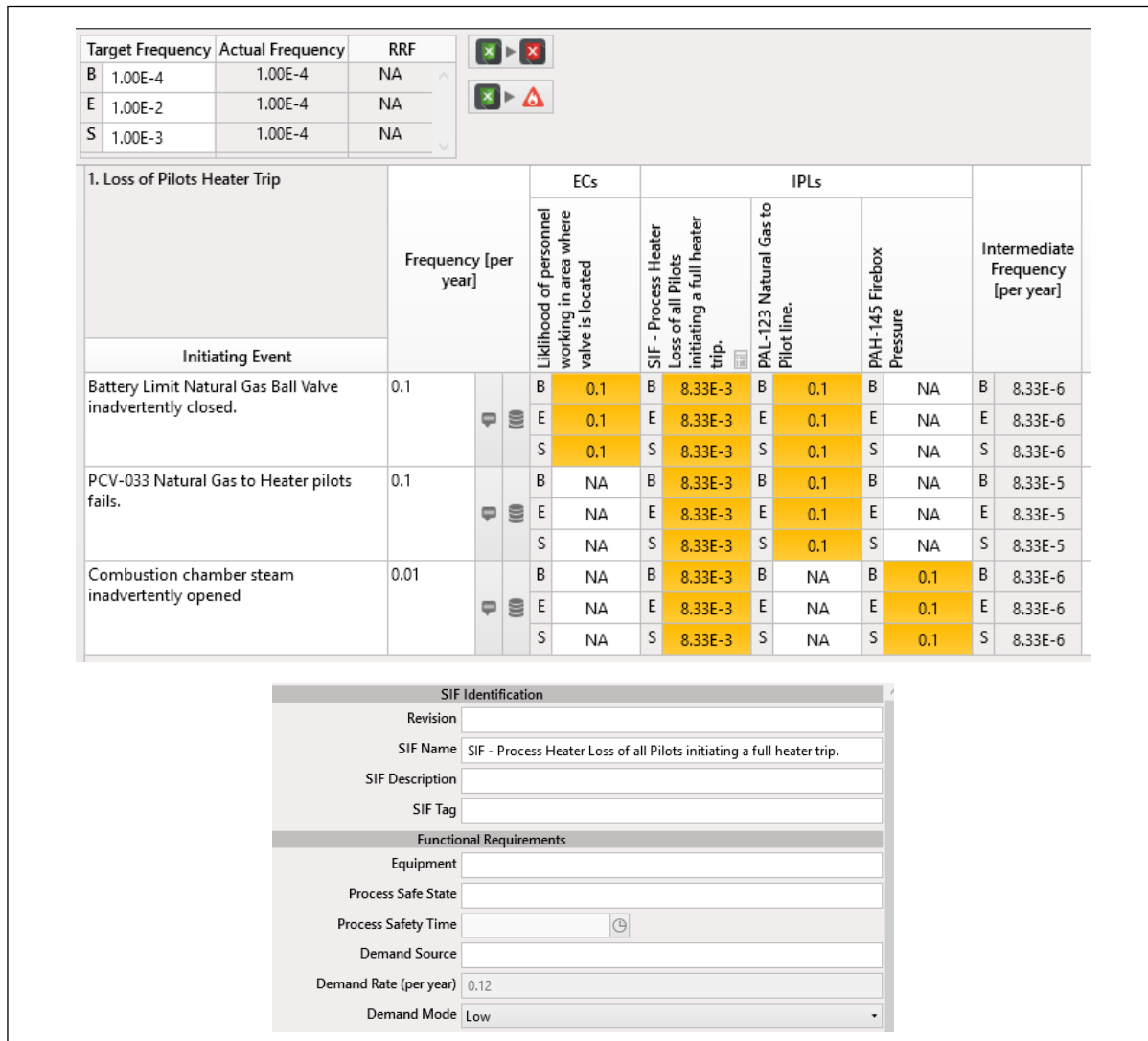


Figure 6 – Combined Evaluation

The analysis yields a combined initiating event frequency of 0.12 demands per year and a SIL 2 target with minimum RRF of 120. Table 2 is a summary comparing the results of the combined analysis to the results of the ‘worst case’ individual analysis from above.

Table 2 – Design Basis Comparison

	SIL Target	SIF PFD target	Demand Frequency / year
Cause 2 design basis (‘worst case’)	2	100	0.1
Combined analysis design basis	2	120	0.12

The comparison in Table 2 demonstrates that the composite LOPA is effective in identifying the impact of multiple initiating events on the overall demand frequency and takes into account the

residual risk, when establishing the SIL target. Considering cause/consequence scenarios separately results in an underestimation of both demand and the required RRF. It is important to note that summing the results of the individual analysis, shown in Table 1, will produce the same result as the combined analysis, unfortunately this step is often overlooked.

Benefit of IPLs that Reduce Demand Frequency

ECs, IPLs and CMs are arranged in the LOPA to consider the impact on initiating event and consequence frequency. This is similar to the approach of the event tree method shown in Figure 1B. The columns should be placed left to right to reflect the expected sequence of events. Figure 3 illustrates the adjustment of initiating event frequency based on the application of an enabling condition. In this example, the valve is located remotely from the process in an area where valves are seldom operated. The use of an EC clearly indicates a reduced likelihood of this initiator (human error) to those reviewing the LOPA at a later date. In this LOPA format, ECs are conditions that impact the initiating event frequency so they always reduce demand and are placed left of the IPLs. Conditional modifiers are conditions that impact the likelihood of a particular outcome once the scenario is initiated. CMs will always appear to the right of the IPLs because they do not impact SIF demand but do impact the potential for worst case consequence.

Within the IPL group, columns are shifted left or right of the SIF based on both scenario development sequence and confidence in the IPL effectiveness to reduce demand. For example, a pressure safety valve (PSV) IPL would be placed to the right of the SIF because the SIF set point is below the relief threshold and the SIF should act before the PSV where a loss of containment consequence is realized. In a scenario where the initiating event is not DCS related (e.g. a human error), response of a DCS control loop may be credited as an IPL and would be placed left of the SIF because it is effective in reducing demand on the SIF.

Operator response to an alarm is an IPL that may be considered to reduce SIF demand, or discounted due to potential ineffectiveness. The efficacy of operator response to an alarm is largely dependent on a facility's alarm management program. A large quantity of alarms, confusing priority (e.g. critical alarm on a situation the operator knows to be minimal risk) and known nuisance alarms (e.g. sensor out of service) can work together to desensitize an operator and increase the likelihood that an operator would fail to respond appropriately to an alarm. Standards like ISA 18.2³ have established a lifecycle framework for alarm management. Figure 7⁴ illustrates experience of one oil and gas producer for two operator consoles before, during and after implementation of ISA 18.2.

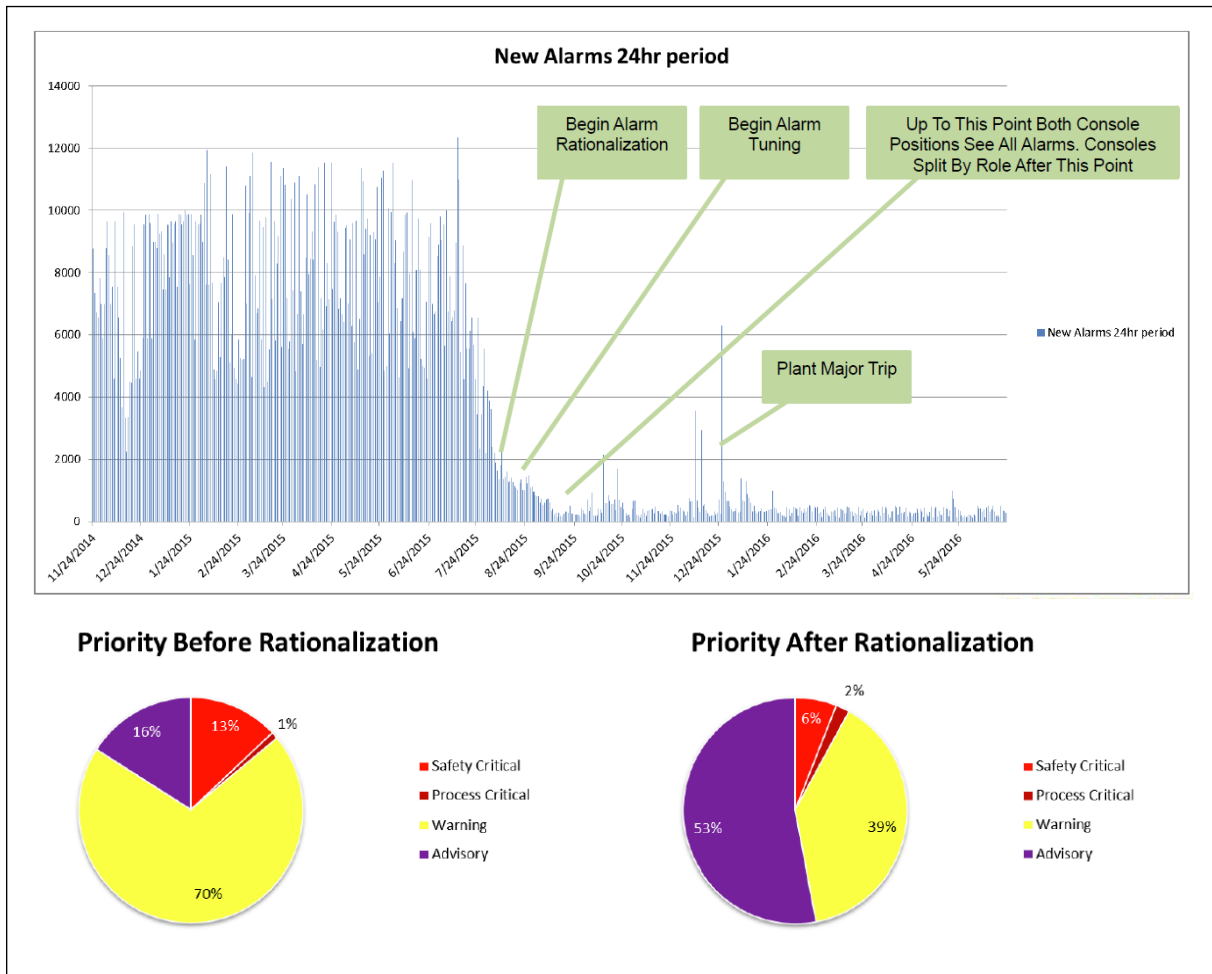


Figure 7 – Impact of ISA 18.2 on Alarm Load and Priority

Before ISA 18.2 implementation, the operators routinely received large numbers of alarms and 70% of the alarms were the same priority. After implementation the operators received significantly fewer alarms, and priority distribution was adjusted to improve visibility of more important alarms. A facility that has implemented an alarm management program, has completed alarm rationalization, utilizes advance alarm groups (flood suppression) and has a routine monitoring program to identify and correct issues, may have more confidence in the effectiveness of the alarm IPL⁵. Such an organization may elect to take credit for this and reduce the design demand rate on SIFs. In the exSILentia tool the alarm IPL columns are shifted left of the SIF and the demand rate calculated for the SRS is adjusted accordingly (Figure 8).

Target Frequency	Actual Frequency	RRF		
B 1.00E-4	1.00E-4	NA		
E 1.00E-2	1.00E-4	NA		
S 1.00E-3	1.00E-4	NA		

6. Loss of Pilots Heater Trip - With Alarm to reduce demand		Frequency [per year]			ECs		IPLs				Intermediate Frequency [per year]	
Initiating Event	Likelihood of personnel working in area where valve is located				PAL-123 Natural Gas to Pilot line.	PAH-145 Firebox Pressure	SIF - with alarm to reduce demand					
Battery Limit Natural Gas Ball Valve inadvertently closed.	0.1	 	B	0.1	B	0.1	B	NA	B	8.33E-3	B	8.33E-6
			E	0.1	E	0.1	E	NA	E	8.33E-3	E	8.33E-6
			S	0.1	S	0.1	S	NA	S	8.33E-3	S	8.33E-6
PCV-033 Natural Gas to Heater pilots fails.	0.1	 	B	NA	B	0.1	B	NA	B	8.33E-3	B	8.33E-5
			E	NA	E	0.1	E	NA	E	8.33E-3	E	8.33E-5
			S	NA	S	0.1	S	NA	S	8.33E-3	S	8.33E-5
Combustion chamber steam inadvertently opened	0.01	 	B	NA	B	NA	B	0.1	B	8.33E-3	B	8.33E-6
			E	NA	E	NA	E	0.1	E	8.33E-3	E	8.33E-6
			S	NA	S	NA	S	0.1	S	8.33E-3	S	8.33E-6

SIF Identification	
Revision	<input type="text"/>
SIF Name	SIF - with alarm to reduce demand
SIF Description	<input type="text"/>
SIF Tag	<input type="text"/>
Functional Requirements	
Equipment	<input type="text"/>
Process Safe State	<input type="text"/>
Process Safety Time	<input type="text"/>
Demand Source	<input type="text"/>
Demand Rate (per year)	0.012
Demand Mode	Low

Figure 8 – Alarm Credit to Reduce Demand Frequency

Demand Mode

It is a common expectation in the process industry that SIFs operate in low demand mode; however, this is not always the case. IEC 61511 2nd edition explicitly states that a SIF is in high demand mode if the demand frequency is greater than once per year, and it suggests that a SIF should be considered high demand if “the failure [of the SIF] is undetected and a demand occurs before the next proof test interval”⁶. It is important for facilities to document every SIF trip and perform periodic analysis to confirm the demand frequency is consistent with design basis.

Demand frequency on a SIF is derived directly from the LOPA; however, additional information is required to determine SIF demand mode. Both demand frequency and proof test interval (PTI)

must be considered when determining SIF demand mode. If a SIF is tested annually, the potential for an undetected SIF component failure is low, and the one-per-year threshold from low to high demand holds. As PTI is increased, the potential for a demand to occur between proof tests is increased. For a SIF to be low demand mode, the initiating event frequency must be less than $1/(2*PTI)^7$. Figure 9 illustrates how demand mode threshold changes as PTI is increased.

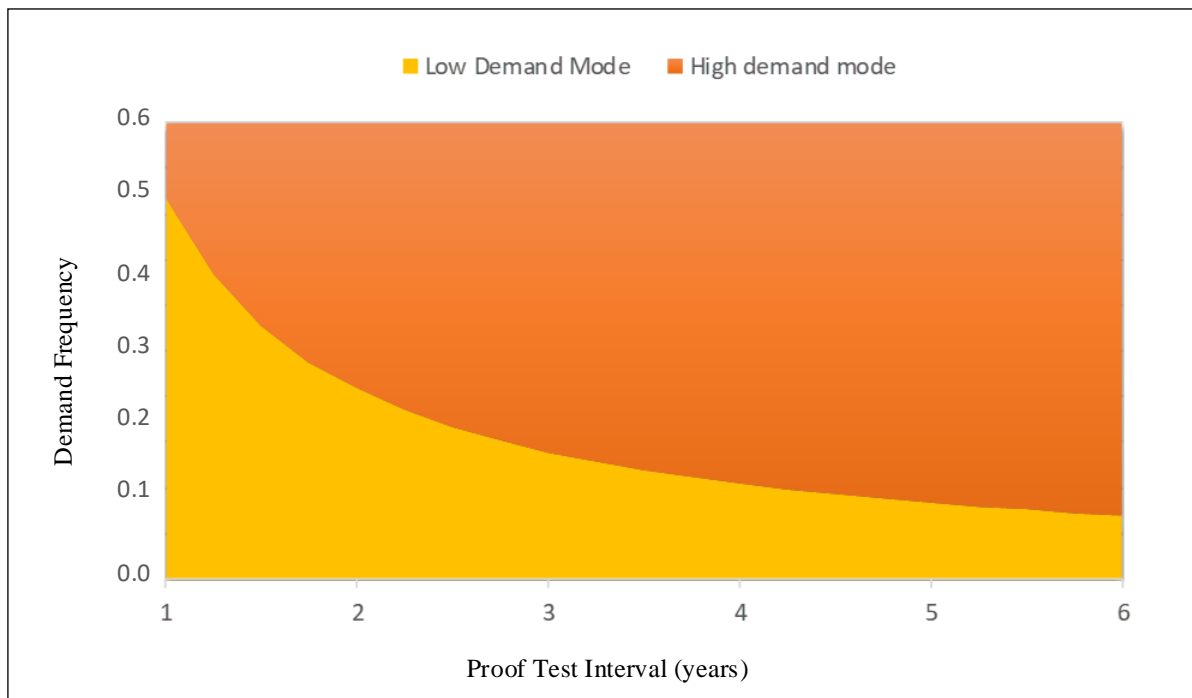


Figure 9 – SIF Demand Mode Threshold

Frequently, processes are designed so they must be shut down to complete proof testing, therefore, often PTI's will correspond to turnaround schedules. As time between turnarounds is increased, the SIFs' PTI is also increased and the SIF can unexpectedly move from low demand mode of operation to high demand mode. If the demand frequency identified in the SRS does not consider all initiating events, a SIF may be believed to operate in low demand mode when it is actually in high demand mode. In high demand mode the effectiveness of proof testing is not achieved, thus the risk reduction provided by the SIF may fall short of requirements and expectations.

Early identification of SIFs that operate in high demand mode provides the most options to resolve back to low demand mode. A SIF may be moved from high to low demand by reducing the frequency of demand or decreasing the proof test interval. Table 3 provides some options:

Table 3 – Demand Reduction Options

Action	Example
Implement administrative program to reduce likelihood of single initiating event	Implement valve locking (carseal) program for manual valves
Reduce failure potential of initiating event through engineering solution	Install two regulators in series rather than one
Install additional instrumentation upstream that will address IEs closer to the source	BPCS or hardwire interlock

Implement programs that improve IPL confidence and reduce demands on SIF	Alarm Management program per ISA 18.2
Reduce proof test interval	Install isolation and bypass capability to permit on line testing

If proof testing can't be implemented for the entire SIF on-line testing, such as partial stroke testing of a valve, can be helpful. Automatic diagnostics with appropriate diagnostics frequency and coverage are required to provide proof testing of high demand mode SIFs.

Conclusion

LOPA is a valuable tool to analyze the risk associated with an event scenario and document the expected effectiveness of protective layers. Many tools are available for conducting the analysis, but few are designed to consider multiple initiating events in a single view as illustrated by the figures above. When using a tool that performs analysis on single cause/consequence pairs, it is necessary to perform an additional step to determine the combined demand frequency and RRF requirement for the SIF. Failure to do so will result in an underestimation of both the initiating event frequency and the RRF target.

When a LOPA is used to determine the design basis for a Safety Instrumented Function (SIF) it is critical that the cumulative effects of multiple initiating events be considered together when assessing IPL effectiveness, and determining the SIF demand frequency and the SIL target. IPLs should be applied only against the initiating events where they are effective thus reducing the residual risk for that scenario. Some IPLs, such as operator response to an alarm, may be considered to reduce the demand rate on a SIF when well managed and monitored by a process such as the ISA 18.2 lifecycle. IPLs should only be considered to reduce SIF demand frequency when they are well managed and monitored to assure effectiveness.

Finally, the proof test interval must be considered to convert demand frequency to demand mode. As intervals between PTI are increased, the potential for hidden failures is increased, thus high demand mode design criteria, including use of diagnostics, is more appropriate. A SIF designed for low demand mode, that is operating in a high demand mode condition is likely to deliver less risk reduction than targeted and may not be effective when called upon to bring the process to a safe state.

¹ Health and Safety Executive, ALARP "at a glance", <http://www.hse.gov.uk/risk/theory/alarpglance.htm>

² exSILentia 4 Integrated Lifecycle Tool, exida.com LLC.

³ Instrument Society of America (ISA), *ANSI/ISA-18.2-2016 Part 1 Management of Alarm Systems for the Process Industries*.

⁴ Benji Kidmose and Jamie Errington, *Austin We Have a Problem*, Emerson Exchange Session 1-9829, 2016

⁵ Todd Stauffer, Nicholas Sands, and David Strobhar, "Closing the Holes in the Swiss Cheese Model"- Maximizing the Reliability of Operator response to Alarms, Global Congress on Process Safety, March 2017.

⁶ IEC 61511-1 Ed 2.0, *Functional Safety: Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements*, IEC, Geneva, Switzerland 2016

⁷ Iwan van Buerden, William M. Goble, *Safety instrumented System Design, Techniques and Design Verification*, Instrument Society of America (ISA), Research Triangle Park, NC, 2018